Dr. Cserépi Judit*:

Mobilfizetés – használjuk vagy féljünk tőle?

Az online pénzügyek és bankkártyás fizetések bővülésével egyre több szolgáltatás jelent meg a digitális világban, melyek talán egyik legnépszerűbb formája a bankkártya digitalizálás, melynek két legismertebb képviselője a piacon a Google Pay és az Apple Pay. Jelen cikkben összegyűjtöttük e mobilfizetési formák előnyeit és hátrányait.

Mi a digitális pénztárca és mire jó?

A Google Pay és Apple Pay alkalmazás digitális pénztárcák (e-pénztárcák, wallet szolgáltatások), melyekkel okostelefonon vagy okosórán is fizethetünk online és személyesen. Android készülékeken a Google Pay, míg IOS rendszerű telefonokon/okos eszközökön az Apple Pay használható. Előnyük, hogy nem kell magunkkal vinni a bankkártyánkat és az arra alkalmas ATM-ben akár pénzt is felvehetünk velük. Például, ha wallet szolgáltatás van az okosóránkon, nyáron azzal fizethetünk és nem kell magunkkal hurcolni a pénztárcát a strandra.

A fizetés biztonságát egy úgynevezett token alapú rendszer garantálja, mely nem adja ki a másik félnek a tényleges bankkártya adatainkat, hanem digitalizálja azokat. A fizetés folyamatában - mind az Apple Pay mind pedig a Google Pay esetén - a két faktoros hitelesítés (további PIN kód, biometrikus azonosító - akár arcfelismerés, ujjlenyomat - megadása a fizetés során) további biztonságot nyújt. Így amennyiben például a strandon elhagyjuk az óránkat, akkor fizetésre más már nem tudja azt felhasználni. Ez alól azonban előfordulhatnak kivételek, például bizonyos esetekben, ha a PIN kód beírása után - annak újbóli megadása nélkül - rövid időn belül több tranzakció is végezhető.

Hogyan digitalizálhatjuk a bankkártyánkat?

Nem minden bankkártya digitalizálható az Apple Pay és a Google Pay alkalmazásokba, ezért érdemes előre tájékozódni a két szolgáltató honlapján és kártyakibocsátó bankunkban. A kártyadigitalizáció egyszerű: először le kell tölteni az applikációt (csak és kizárólag hivatalos forrásból), majd banki mobilapplikáción vagy Apple Pay/Google Pay alkalmazáson keresztül indítható a digitalizálás folyamata. Ezután meg kell adni a bankkártyánk adatait (bankkártya szám, lejárat és CVC/CVV kód). A legfontosabb lépés mégis az, hogy a bankunk azonosítson minket, melyhez egy kódot küld SMS-ben. E kód alkalmazásba történő beírásával véglegesíthetjük a regisztrációt és választhatunk hitelesítési módot (PIN kód, biometrikus adatok) a fizetéshez. A sikeres regisztrációról általában küld a bankunk egy visszaigazoló SMS-t. Természetesen a folyamat véglegesítéséhez igénybe vehetjük a kártyakibocsátó bankunk telefonos ügyfélszolgálatát is.

Hogyan használják ki a csalók a digitalizálás folyamatát?

Bár a kártyadigitalizáció jelenlegi ismereteink szerint biztonságos, a csalók adathalász módszerekkel próbálják megszerezni a bankkártya adatainkat és az SMS-ben küldött banki kódokat. A csalók pszichológiai manipuláció segítségével, adathalász technikákat alkalmazva érik el azt, hogy megkaphassák ezeket az információkat. Ilyen lehet egy SMS, e-mail, hamis webshop, bármilyen hamis weboldal, felhívás nyereményjátékra közösségi oldalakon, vagy pedig telefonhívás.

Például a bűnözők azt állítják, hogy a Netflix alkalmazásba újra meg kell adni a kártyánk adatait, vagy pedig valamilyen számlát kell kifizetnünk a gáz vagy villanyszolgáltatónk részére. Sőt előfordulhat, hogy az adathalászok olyan üzenetet küldenek, hogy postai címadatainkat módosítsuk, mert csomag érkezik részünkre, vagy szabálysértési bírság fizetésében elmaradásunk van. A trükkök sora végtelen. A lényeg az, hogy megszemélyesítenek olyan, általunk ismert szolgáltatókat vagy személyeket - akár a saját bankunkat is - amelyekben bízunk, és azt a látszatot keltik, hogy a szokásos csatornán keresztül a szokásos módon kommunikálnak velünk. Valójában a kártyaadataink és a saját bankunk által küldött SMS kód megszerzése a cél.

Az MNB-ben működő Pénzügyi Békéltető Testület (PBT) előtt tárgyalt ügyek között volt olyan áldozat, aki egy ismert cipőmárka webshopján keresztül szeretett volna vásárolni, viszont nem vette észre, hogy egy adathalász áloldalon adta le a rendelését (egyúttal bankkártya adatait). Ezután egy Apple Pay regisztrációhoz szükséges SMS üzenetet kapott, melyet nem olvasott el figyelmesen, csupán a benne található kódra figyelt, melyet meg is adott a vásárláshoz. Később bankkártyájával általa jóvá nem hagyott tranzakciók történtek. Tehát, ha egy csaló megszerzi a kártyaadatainkat és az SMS-ben kapott kódot, akkor regisztrálhatja bankkártyánkat saját eszközére és később vásárolhat vele. Egy másik esetben Google Pay regisztrációhoz szükséges kóddal történt visszaélés, ahol a csalók a regisztrációt követően csak két héttel később használták az alkalmazást vásárlásra.

A PBT tapasztalatai alapján az a közös az Apple Pay és Google Pay regisztrációs ügyekben, hogy amennyiben a fogyasztók nem adták volna meg az SMS kódot vagy nem tették volna elérhetővé, a csalók csupán a bankkártyaadatokkal valószínűleg nem tudtak volna kárt okozni. Ezen esetek nagy része megelőzhető lenne azzal, ha az emberek elolvasnák az SMS-ek szövegét és nem rutinból cselekednének. Ha pedig nem értik a kapott üzenetet - mert például nem hallottak az Apple Pay és Google Payről, vagy az angolul érkezik - akkor se adják meg az SMS kódot sehol és senkinek.

Ha mégis megadtuk az SMS kódot, azonnal bejelentést kell tenni a bankunknak és a bankkártyánkat le kell tiltani. Érdemes rendőrségi feljelentést is tenni az ügy kapcsán. Ne bízzunk abban, hogy a figyelmetlenség ellenére talán mégsem történik semmi, mert a tapasztalat azt mutatja, hogy napokkal, hetekkel később is elkezdődhetnek az általunk jóvá nem hagyott kártyás tranzakciók. Ez azokra az esetekre is vonatkozik, amikor látunk Google Pay/Apple Pay regisztrációs SMS-t a telefonunkon, azonban nem tudjuk felidézni, hogy azt miért kaptuk, vagy bárhol megadhattuk volna.

Nagyon gyakran a csalók épp olyan időszakban küldenek adathalász e-maileket vagy SMS-eket (például arról, hogy csomagunk érkezett, de vámot kell fizetni), amikor ünnepi időszak van és mindenki csomagot vár, vagy például egy pénteki napon, kihasználva, hogy a hétvégén kisebb kapacitással működnek a bankok telefonos ügyfélszolgálatai és személyes ügyintézésre sincs általában hétvégén lehetőség.

Íme néhány jó tanács mire figyeljünk!

- Csak és kizárólag hivatalos forrásból, a Google Pay esetén a Play áruházból vagy Apple Pay esetén az Apple Store-ból töltsük le az applikációkat;
- Mindig ellenőrizzük, hogy megfelelő banki oldalon, webshop oldalán vásárlunk és adjuk meg a bankkártya adatainkat;

- Ha kapunk egy SMS-t vagy e-mailt egy linkkel, azokat mindig óvatosan kezeljük, ne klikkeljünk rájuk, csak miután ellenőriztük, hogy azok tényleg az ismert szolgáltatótól érkeztek;
- Ha siettetnek egy levélben, mert például fizetési elmaradásunk van, akkor mindig gyanakodjunk és nézzünk utána;
- Ha telefonhívást kapunk a bankunk nevében, kérdezzük meg a hívó felet, hogy milyen ügyben keres bennünket, majd tájékoztassuk, hogy a bankunk ügyfélszolgálatát fogjuk visszahívni és szakítsuk meg a vonalat. Ezután érdemes a bankunk hivatalos ügyfélszolgálati telefonszámán érdeklődni, hogy az adott ügyben tényleg ők kerestek-e minket.
- Ha SMS üzenetet várunk a bankunktól (például vásárlás jóváhagyásához), de más tartalmú üzenetet kapunk (például Apple Pay regisztrációhoz vagy angol nyelvű üzenetet kapunk), akkor szakítsuk meg a folyamatot és ne adjuk meg a kapott kódot sehol, senkinek;
- Ne adjuk meg sem bankkártya adatainkat, SMS-ben érkezett kódokat másoknak telefonon, chat felületen és egyéb kommunikációs csatornán keresztül;
- Ne olvassunk be olyan QR kódot telefonunk mobilapplikációja segítségével, ami chat felületen, SMS-ben ismeretlen harmadik személy küldött vagy egy olyan személynek, aki egy adott bank munkatársának adja ki magát;
- Amennyiben Androidos telefonunk van és Apple Pay regisztrációs kódot tartalmazó SMS-t kapunk (vagy fordítva), akkor azonnal vegyük fel a kapcsolatot a bankunkkal, illetve ne adjuk meg a kódot senkinek;
- Ha online vásárlásunk során nem kapunk a fizetésről visszaigazolást, akkor is érdemes gyanakodnunk, hogy csalás áldozatává váltunk;
- Mindig gyanúra adjon okot, ha külföldi számról hívnak, illetve, ha ugyan belföldi számról, de azt nem tudjuk visszahívni, mert ilyen előfizető nem létezik;
- Érdemes vásárlási limiteket beállítani, melyeket egy-egy tervezett nagyobb összegű vásárlás előtt ideiglenesen felemelhetünk, majd vissza is állíthatunk;
- Kísérjük figyelemmel naponta a költéseinket, a pénzügyi tranzakcióinkat, lehetőleg legyen kártya, illetve számlakontroll szolgáltatásunk beállítva;
- Soha ne töltsünk le kérésre távoli hozzáférést biztosító szoftvert eszközeinkre harmadik, ismeretlen személyek kérésére.

Az Apple Pay és Google Pay két népszerű, egyszerű és kényelmes alkalmazás, de óvatosságot igényelnek az adathalászat és csalások miatt. Ezen kívül technikai problémák is előfordulhatnak, mint ahogy az Apple Pay-nél is fellépett a magyar ügyfeleket érintően 2024. június 26-án, melynek során nagy mennyiségű, az ügyfelek által jóvá nem hagyott tranzakció valósult meg.

Figyeljünk oda, és tartsuk szem előtt a biztonságot, melyhez a kulcs a saját kezünkben van. Ha bizonytalanok vagyunk, mindig konzultáljunk bankunkkal. További információért érdemes ellátogatni a https://kiberpajzs.hu/ weboldalra, ahol rendszeres tájékoztatást és tanácsokat kaphatunk az épp aktuális csalási trendekről és azok elkerülési módjairól.

** A szerző a Magyar Nemzeti Bank mellett működő Pénzügyi Békéltető Testület tagja*
„Szerkesztett formában megjelent 2024. december 18-án a VG oldalon."